Remarks/Arguments:

As of the Action, Claims 2-4 and 6-28 are pending in the Application. All Claims stand rejected.

By this filing, Applicant responds to the Action. Applicant herein amends Claim 28. Applicant adds no new matter.

In view of the Claims as set forth above and the remarks below, Applicant respectfully requests reconsideration and further examination of this Application.

Rejections of Claims under Section 112, First Paragraph: The Action rejects Claim 28 for recitation of the "temperature, or other indirect radiation" limitation, based on the argument that this subject matter "was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention." Specifically, the Action argues that the specification does not disclosure that consumption characteristics are based on temperature or other forms of indirect radiation".

Applicant notes that "indirect radiation" is explicitly mentioned in the discussion of Differential Power Analysis, on page 2, line 23. Applicant submits that this recitation of "indirect radiation", in the context of Differential Power Analysis and the other disclosures of this Application, fully meets requirements of Section 112, first paragraph.

Applicant has also amended Claim 28 so as to expand the scope of the claim to include recitations to "voltage and "fluctuations and other timing characteristics". In doing so, Applicant adds no new matter, as this additional subject matter is referenced variously in the Application, including on page 2, lines 23-31.

In view of the foregoing, Applicant requests that these rejections be reconsidered and withdrawn.

Rejections of Claims Based on Ugon: The Action rejects all Claims under 35 U.S.C. §102(e) or §103(a) as being, respectively, anticipated by Ugon et al, U.S. Patent No. 6,839,849 ("Ugon"), and unpatentable over Ugon in view of Official Notice or various other cited references.

The Action notes that Applicant cannot rely upon its foreign priority papers to overcome these rejections because a translation of said papers has not been made of record in accordance with 37 C.F.R. 1.55.

Applicant notes that the certified copy of the German patent application to which this Application claims priority is of record in the file.

Applicant files, concurrently herewith, an English-language translation of the previously-filed certified copy, together with a statement that the translation is accurate.

In view of the foregoing, Applicant requests that these rejections be reconsidered and withdrawn.

Rejections of Claims Based on Patarin In View of Jahnich and Tan: The Action maintains the previous rejections of Claims 2-4 and 6-14 under 35 U.S.C. §103(a) as being unpatentable over Patarin et al U.S. Patent No. 6,658,569 ("Patarin") in view of, variously, Jahnich and Tan.

In response to these rejections, Applicant re-asserts here the arguments presented in the filing of 14 July 2005. (Applicant so re-asserts by reference only, electing to omit physical duplication of the arguments toward conserving natural resources, communication resources, file space and the like.) However, for emphasis, Applicant submits here:

a) Nowhere does the Action set forth suggestion or motivation in Patarin, Jahnich or Tan to properly support the Action's conclusion that it would be obvious to modify Patarin based on Jahnich or Tan.

b) The Action gathers various parts from Patarin, Jahnich and Tan, doing so based solely on Applicant's Claims and teachings (i.e., using the Application as a "road map") and, ultimately, toward listing the elements recited in Applicant's Claims.

c) Even assuming that the Action gathers parts from cited references so as to successfully list all elements of Applicant's Claims, nowhere does the Action address arranging the gathered parts and, in particular, nowhere does the Action deal with (i) the de-motivation to combine that arises from Patarin's complexity and (ii) the absence of any reasonable expectation of success attendant to Patarin's complexity (i.e., such complexity raises clear issues as to whether Patarin can be modified at all, let alone how or whether any of it could be successful, even when using Applicant's Claims and teachings as a "road map").

d) Even with the Action directed to gathering parts toward listing elements of Applicant's Claims, nowhere does the Action succeed in gathering a part that meets Applicant's element/arrangement in re dummy operations that run simultaneously and in parallel with useful operations using at least two processors (e.g., rather than dummy operations that run in parallel, the Action cites to Jahnich, pointing to sections in Jahnich so as to find some/any kind of dummy operations, while also being blind to the limitation that these operations are expressly described as being "permuted" into serial execution with the useful operations).

e) Even with the Action directed to gathering parts toward listing elements of Applicant's Claims, nowhere does the Action succeed in gathering a

part that meets Applicant's element/arrangement in re randomization in selection of processors or splitting of useful operations as to a particular useful operation, in handling DPA (e.g., rather than randomization consistent with Applicant's elements, the Action cites to Tan, pointing to sections in Tan so as to find some/any kind of randomization, while being blind to the limitation that these operations are expressly described as being to create an cryptography algorithm from among a multitude of possible such algorithms, and not for dealing with DPA as to a selected cryptography operation).

In addition, Applicant herewith re-iterates the remarks set forth in its previous responses, filed 16 December 2004).

In view of the foregoing, Applicant requests that these rejections be reconsidered and withdrawn.

Rejections of Claims Based on Patarin In View of Ohki: The Action rejects claims 15-18, 20-26 and 28 under 35 USC 103(a) as unpatentable over Patarin in view of Ohki et al, U.S. Patent No. 6,839,847 ("Ohki").

The Action states that Patarin does not disclose a "second operation associated with consumption characteristics complementary to consumption characteristics associated with the cryptographic operation." To fill this stated gap in Patarin, the Action relies on Ohki. Specifically, the Action alleges that Ohki discloses a device performing two operations: a cryptographic operation using normal input data and another operation using inverted input data, such that the power consumption of the device remains constant (citing to Ohki at Col. 2, Line 36 – Col. 3, Line 6).

Applicant submits that the Action fails to establish a prima facie case to support this obviousness rejection. To properly establish a prima facie case of obviousness, the Action must establish three basic criteria. First, the Action must identify suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, which supports modifying the references or combining the references' teachings. Second, in so modifying/combining, a reasonable expectation of success must exist. Third, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Even with these criteria met, the Action may establish a prima facie case of obviousness only if the teaching or suggestion to make the combination/modification and the reasonable expectation of success are both found in the prior art, rather than being based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Here, the Action does not meet the three criteria, and the combinations/modifications appear to be based on applicant's disclosure.

To illustrate, the Action omits to identify where Patarin discloses, or even contemplates, operations performed "simultaneously and in parallel" so that "consumption characteristics of the data-processing device is a superposition", as claimed in all these rejected Claims. (Indeed, as to Patarin, Applicant hereby re-iterates the arguments presented in the filing of 14 July 2005, doing so by reference only.)

To illustrate further, even assuming that the Action's citations as to Ohki provide the disclosures alleged in the Action, the Action fails to provide proper suggestion or motivation to do so. That is, nowhere does the Action set forth any sufficient suggestion or motivation from Patarin or Ohki to support the Action's conclusion that it would be obvious to modify Patarin's complex process to use the dummy programs of Jahnich. Indeed, the Action appears to combine solely based on, and so as merely to assemble the elements of, Applicant's Claims.

Indeed, nowhere does the Action describe how Patarin's process would/could be modified to combine anything from Ohki. Given the complexity of the Patarin process, there is

no basis for a "reasonable expectation of success" in any such combination. That is, Patarin's complexity raises clear issues as to whether Patarin can be modified at all, let alone how or whether any of it could be successful, even when using Applicant's Claims and teachings as a "road map"). Even so, the Action omits to address the absence of an expectation of success.

In view of the foregoing, Applicant requests that these rejections be reconsidered and withdrawn.

CONCLUSION

Generally, in this Amendment and Response, Applicant has not raised all possible grounds for (a) traversing the rejections of the Action or (b) patentably distinguishing the new Claims (i.e., over the cited references or otherwise). Applicant, however, reserves the right to explicate and expand on any ground already raised and/or to raise other grounds for traversing and/or for distinguishing, including, without limitation, by explaining and/or distinguishing the subject matter of the Application and/or any cited reference at a later time (e.g., in the event that this Application does not proceed to issue with the Claims as herein amended, or in the context of a continuing application). Applicant submits that nothing herein is, or should be deemed to be, a disclaimer of any rights, acquiescence in any rejection, or a waiver of any arguments that might have been raised but were not raised herein, or otherwise in the prosecution of this Application, whether as to the original Claims or as to any of the new Claims, or otherwise. Without limiting the generality of the foregoing, Applicant reserves the right to reintroduce one or more of the original Claims in original form or otherwise so as to claim the subject matter of those Claims, both/either at a later time in prosecuting this Application or in the context of a continuing application.

Applicant submits that, in view of the foregoing remarks and/or amendments, the Application is in condition for allowance, and respectfully requests reconsideration and favorable action.

The Commissioner is hereby authorized to charge any fees (including extension fees), additional fees, or underpayments, or to credit any overpayments, to the undersigned attorney's Deposit Account No. 50-1001; provided, however, that such fees, underpayments or overpayments must arise solely in connection with this Amendment and Response. Otherwise, the Commissioner should review and follow any authorization previously given by Applicant to charge certain such fees and credit certain such overpayments to the Applicant's separate Deposit Account (No. 14-1270).

Respectfully submitted,

Date: December 30, 2005

Michael E. Schmitt
Registration No. 36,921
P. O. Box 2200
Hillsboro, OR 97123
Telephone: (503) 844-9009
Facsimile: (503) 296-2172

Correspondence to:

Philips Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131 USA
Telephone: (408) 474-9073
Facsimile: (408) 474-9082
USPTO Customer Number: 24738